MATH 25 CLASS 5 NOTES, SEP 30 2011

Contents

Quick links to definitions/theorems

- Euclid's Lemma (important!)

1. A brief diversion: relatively prime numbers

Before continuing with the study of linear equations, we make a brief detour to talk about some useful properties of relatively prime numbers and a number related to gcds.

Recall that two integers a, b are relatively prime if $\gcd(a, b) = 1$. At this point, we know enough to prove some very important facts about relatively prime numbers:

Proposition 1. *Let a, b be two relatively prime numbers, and let c be some integer. If $a \mid bc$, then $a \mid c$.*

Proof. We know that $a \mid bc$. Because a, b are relatively prime, we know that $ax+by = 1$ has (infinitely) many integer solutions. Select one of them. Multiply this equation by c: $acx + bcy = c$. Notice that $a \mid acx$, and since $a \mid bc$ by assumption, $a \mid bcy$. Therefore, $a \mid c$. $\square$

This simple result is of fundamental importance. Notice that we used our knowledge about when $ax + by = d$ has solutions in an essential way to prove this proposition. Another important observation is that the above proposition requires that a, b be relatively prime in order to be true. Can you think of an example where a, b are not relatively prime, and where $a \mid bc$ but $a \nmid c$?

Finally, one special case of the above proposition deserves mention. Suppose $a = p$ is a prime number (a number divisible only by 1 and itself). Then the above proposition can be rewritten in the following way:

Lemma 1 (Euclid's Lemma)**.** *Let p be a prime, and let a, b be two integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, there is nothing to prove, so suppose $p \nmid a$. Then $\gcd(a, p) = 1$, since the only divisors of p are 1 and p, while p does not divide a. An application of the previous proposition shows that $p \mid b$. $\square$

Example. This example shows that the original proposition (and Euclid's Lemma) can be false when their assumptions are not true. For instance, if $a = 4, b = 6$, so that $\gcd(a, b) = 2$, then we can choose $c = 2$. Then $bc = 12$, so $a \mid bc$, but $a \nmid c$. This example also works to show why p must be prime in Euclid's Lemma; notice that $a = 4$ is not a prime, yet $a \nmid b, c$.

The previous proposition and lemma are one of the most important applications of our knowledge of when $ax + by = d$ has integer solutions. It is well worth learning their statements and proofs thoroughly. Here are several other useful propositions:

Proposition 2 (Corollary 1.11a of the text)**.** *If a, b are relatively prime integers, and $a \mid c, b \mid c$, then $ab \mid c$.*

Proof. Since $\gcd(a, b) = 1$, there exist integers x, y such that $ax + by = 1$. Multiply this equation by $c : acx + bcy = c$. Since $b \mid c, (ab) \mid acx$, and since $a \mid c, (ab) \mid bcy$. Therefore $(ab) \mid c$. □

Proposition 3. *[Exercise 1.8 of the text] Let a, b be two integers. If c is a divisor of a, b, then $c \mid \gcd(a, b)$.*

Proof. We know that there is a pair of integers x, y such that $ax + by = \gcd(a, b)$. Since $c \mid a, b$, this implies that $c \mid \gcd(a, b)$. □

Proposition 4 (Corollary 1.10 of the text)**.** *Let a, b be two integers, and let m be a positive integer. Then $\gcd(ma, mb) = m \gcd(a, b)$.*

Proof. Clearly $m \gcd(a, b) \leq \gcd(ma, mb)$, because $m \gcd(a, b)$ divides both ma and mb. For the reverse inequality, again there are two integers x, y such that $ax + by = \gcd(a, b)$. Multiplying this equation by m, we get $max + mby = m \gcd(a, b)$. However, this is only possible if $\gcd(ma, mb) \mid m \gcd(a, b)$, which in particular implies that $\gcd(ma, mb) \leq m \gcd(a, b)$, as desired. □

Proposition 5 (Corollary 1.10 of the text)**.** *Let a, b be two integers, and let $d \mid a, b$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = \frac{\gcd(a, b)}{d}$. In particular, $\frac{a}{\gcd(a, b)}$ and $\frac{b}{\gcd(a, b)}$ are relatively prime.*

Proof. Again, there exist integers x, y which satisfy $ax + by = \gcd(a, b)$. Divide this equation by d:

$$\frac{a}{d}x + \frac{b}{d}y = \frac{\gcd(a, b)}{d}.$$

Since $a/d, b/d$ are integers, this says that $\gcd(a/d, b/d) \leq \gcd(a, b)/d$. On the other hand since $\gcd(a, b) \mid a, b$, $\gcd(a, b)/d \mid a/d, b/d$. So $\gcd(a, b)/d \leq \gcd(a/d, b/d)$, and therefore we have equality. □

As you can see, we are getting a lot of mileage out of the fact that $ax + by = d$ has integer solutions x, y if and only if $\gcd(a, b) \mid d$. Let's conclude this section with an example illustrating these propositions.

Examples.

- We saw that $\gcd(994, 399) = 7$. Therefore, the only common divisors of $994, 399$ are $1, 7$ (Proposition 3). As $994 = 7 \cdot 142, 399 = 7 \cdot 57$, we also see that $\gcd(142, 57) = 1$. (Proposition 5)
- Proposition 2 can be false if $\gcd(a, b) \neq 1$. For instance, if $a = 6, b = 9$, and $c = 18$, then $a \mid c, b \mid c$, but $ab = 54 \nmid c$.

2. Least common multiples

Recall that a *multiple* of an integer a is any number of the form na, where $n \in \mathbb{Z}$. Given two numbers a, b, we call the smallest positive integer which is both a multiple of a, b the *least common multiple* of a, b. This number is often written $\operatorname{lcm}(a, b)$, or sometimes $[a, b]$, although again the latter notation can be ambiguous, since it also means the closed interval from a to b. There is the obvious generalization of this definition to a list of more than two numbers.

Example. Let $a = 8, b = 12$. Then the least common multiple of a, b is 24, since 24 is the smallest number that is a multiple of both a, b.

How are the lcm and gcd of two nonzero numbers a, b related? Notice that $\gcd(8, 12) = 4$, for example. A bit of experimentation will probably lead you to the claim that $\gcd(a, b)\operatorname{lcm}(a, b) = |a||b|$. Let's prove this:

Proof. We can assume that a, b are positive, since gcd, lcm are unchanged if we change the signs of a, b. First notice that because $\gcd(a, b) \mid a, b$, we know that $a/\gcd(a, b)$ is an integer, and similarly, $b/\gcd(a, b)$ is an integer. Therefore,

$$\frac{a}{\gcd(a,b)}b = \frac{b}{\gcd(a,b)}a = \frac{ab}{\gcd(a,b)}$$

shows that $ab/(\gcd(a, b))$ is a common multiple of a, b. Therefore, $\operatorname{lcm}(a, b) \leq ab/(\gcd(a, b))$.

Now we want to show that the opposite inequality is true. Suppose that c is the least common multiple of a, b. Then we can write $c = an = bm$ for some integers n, m. In particular, this means that $n \mid bm, m \mid an$. First notice that $\gcd(n, m) = 1$. This must be true because if $\gcd(n, m) > 1$, then we can divide both n, m by their gcds to obtain new integers n', m', with $(n', m') = 1$, and $an' = bm'$ is still a common multiple of a, b which is smaller than c, contradicting the fact that c is the least common multiple of a, b.

Since $\gcd(n, m) = 1$, we can apply the first proposition we learned to see that $n \mid b, m \mid a$. Let $a_1 = a/m, b_1 = b/n$. However, we know that $an = bm$, so this tells us that $a_1 = b_1$. Call this number d. Notice that d is a common divisor of a, b. Therefore, $d \leq \gcd(a, b)$. But this implies that

$$\frac{ab}{d} \geq \frac{ab}{\gcd(a,b)}.$$

Since $ab/d = c$, this shows that $c \geq ab/(\gcd(a, b))$ as desired. Putting the two inequalities we've proved together, we have $c = ab/(\gcd(a, b))$, as desired. $\square$

Example. Going back to $a = 994, b = 399$, since $\gcd(994, 399) = 7, \operatorname{lcm}(994, 399) = 994 \cdot 399/7 = 56658$.

We conclude with a proposition which is the mirror image of Proposition 3.

Proposition 6 (Exercise 1.14 of the text)**.** *Let c be a common multiple of a, b. Then c is a multiple of* $\operatorname{lcm}(a, b)$.

Proof. Write $\ell = \operatorname{lcm}(a, b)$. Since $c \geq \ell$, a Euclidean division of c by ℓ gives an equation $c = \ell q + r$, where $0 \leq r < \ell$. But since $a, b \mid c, \ell$, this means $a, b \mid r$, which shows that r is a common multiple of a, b. Since ℓ is the least common multiple, we must have $r = 0$, which means that c is a multiple of $\ell = \operatorname{lcm}(a, b)$, as desired. □

The converse to the above proposition is obviously true – that is, any multiple of $\operatorname{lcm}(a, b)$ is itself a common multiple of a and b. Let's conclude by going back to a familiar example.

Example. We calculated that $\operatorname{lcm}(994, 399) = 56658$. Therefore any common multiple of 994 and 399 is a multiple of 56658.

3. Finding all solutions to $ax + by = c$

The Euclidean algorithm gives us a way to find a pair of integer solutions x, y to $ax + by = c$, as long as $\gcd(a, b) \mid c$. However, it would be ideal to know how to find all the solutions to this equation, instead of just one. The following proposition tells us just how to do this:

Proposition 7 (Theorem 1.13 of the text)**.** *Let a, b be nonzero integers, and c an integer which is a multiple of* $\gcd(a, b) = d$. *Let x_0, y_0 be one pair of integer solutions to $ax + by = c$. Then the set of all integer solutions x, y to the equation $ax + by = c$ has the form*

$$x = x_0 + \frac{b}{d} n, y = y_0 - \frac{a}{d} n, \tag{1}$$

where n is any integer. (In particular when $n = 0$ we get the initial pair x_0, y_0.)

Proof. We will begin by checking that every pair of integers x, y satisfying Equation 1 satisfies $ax + by = c$. Plug in the two equations from Equation 1 into $ax + by = c$:

$$a\left(x_0 + \frac{b}{d} n\right) + b\left(y_0 - \frac{a}{d} n\right) = ax_0 + \frac{ab}{d} n + by_0 - \frac{ab}{d} n = ax_0 + by_0 = c.$$

In the last equality, we used the fact that x_0, y_0 was a solution to $ax + by = c$.

We now want to prove the converse statement, that any solution x, y is of the form given by Equation 1. So suppose x, y are integers such that $ax + by = c$. Since $ax_0 + by_0 = c$ as well, we have

$$ax_0 + by_0 = ax + by, \text{or } a(x_0 - x) = b(y - y_0).$$

Both sides are divisible by $d = \gcd(a, b)$, so divide both sides of this equation by d:

$$\frac{a}{d}(x_0 - x) = \frac{b}{d}(y - y_0).$$

Recall that $a/d, b/d$ are relatively prime. Since $a/d, b/d$ are relatively prime and $(b/d) \mid (a/d)(x - x_0)$, we must have $(b/d) \mid (x - x_0)$. In other words, there is an integer n such that

$$\frac{b}{d}n = x - x_0, \text{or } x = x_0 + \frac{b}{d}n.$$

Plugging in this expression for x into the previous equation, we obtain

$$\frac{a}{d}\frac{-b}{d}n = \frac{b}{d}(y - y_0).$$

Solving for y, we get

$$y = y_0 - \frac{a}{d}n.$$

□

Examples.

- Going to our favorite example of $a = 994, b = 399$, we found the solution $x = -2, y = 5$ to $994x + 399y = 7$. Since $\gcd(a, b) = d = 7$, and $a/d = 142, b/d = 57$, the previous proposition tells us that every solution to $994x + 399y = 7$ is given by $x = -2 + 57n, y = 5 - 142n$, where $n \in \mathbb{Z}$.
- Notice that this proposition works on the equation $ax + by = c$ even when c is larger than $\gcd(a, b)$. For example, consider the equation $4x + 6y = 4$. It is obvious that $x = 1, y = 0$ gives an integer solution. We have $a = 4, b = 6, \gcd(a, b) = d = 2$, so $a/d = 2, b/d = 3$. Then the previous proposition tells us that every pair of integer solutions has the form $x = 1 + 3n, y = -2n$.
- In general, it is easy to check your answer by plugging in your expressions for x, y into the equation $ax + by = c$ and checking that you get a true equation. In particular, any ns which appear should end up canceling out.